2014

Resilient Digital Image Watermarking for Document Authentication

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Oleksandr Iakovenko

Recommended Citation

Blackledge, J.M. & Iakovenko, O. (2014) Resilient Digital Image Watermarking for Document Authentication, *IAENG, International Journal of Computer Science,* Vol. 41, No. 1, 1-17, 2014. doi:10.21427/ky8g-6525

Resilient Digital Image Watermarking for Document Authentication

Jonathan Blackledge and Oleksandr Iakovenko

***Abstract*—We consider the applications of the Discrete Cosine Transform (DCT) and then a Chirp coding method for producing a highly robust system for watermarking images using a block partitioning approach subject to a self-alignment strategy and bit error correction. The applications for the algorithms presented and the system developed include the copyright protection of images and Digital Right Management for image libraries, for example. However, the principal focus of the research reported in this paper is on the use of print-scan and e-display-scan image authentication for use in e-tickets where QR code, for example, are embedded in a full colour image of the ticket holder. This requires that an embedding procedure is developed that is highly robust to blur, noise, geometric distortions such as rotation, shift and barrel and the partial removal of image segments, all of which are considered in regard to the resilience of the method proposed and its practical realisation in a real operating environment.**

***Index Terms*—Resilient Watermarking, DCT, Chirp Coding, Block Embedding, Binary Information Hiding**

I. Introduction

THE watermarking of digital images has become a common concern with regard to copyright protection and Digital Rights Management. The principal aim is to design algorithms which provide for the authentication of single and/or multiple image frames by hiding information in an image that is encrypted or otherwise [1]. A large amount of copyright information now resides in the form of digital images especially with regard to the growth of electronic publishing. Moreover, the future of networked multimedia systems is becoming increasingly conditioned by the development of efficient methods to protect ownership rights against unauthorised copying and redistribution. Digital image watermarking has emerged as a candidate to solve this problem and since the mid-1990s there has been a convergence of a number of different information protection technologies whose theme is hiding (as opposed to encrypting) digital information. In this context, we present a brief introduction on watermarking and Steganography which is given in the following section.

A. Watermarking and Steganography

Information hiding can refer to either making additional information imperceptible or keeping the existence of the information secret. Important sub-disciplines of information hiding are *Steganography* and watermarking which are concerned with techniques that are used to imperceptibly convey information. However, they are two different and distinct disciplines. Watermarking is the practice of hiding an information source (copyright information, for example) in a signal or image without degrading its quality in such a way that it is expected to be permanently embedded into the data and can be detected at a later time. Steganography is the study of the techniques used to hide one message inside another, without disclosing the existence of the hidden message or making it apparent to an observer that it exists. Digital image watermarking and Steganography are thus distinguished from each other as follows (e.g. [2], [3] and [4]):

1) Steganography is the 'art' of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message whereas the information hidden by a digital watermarking system (which can also refer to the application of visible watermarks, commonly used to protect image samples, for example, from unauthorised use) is always associated with the object to be protected or its owner (Steganographic systems focusing on just hiding information).
2) The purpose of Steganography is to provide for the covert communication between two parties whose existence is unknown to a possible attacker, a successful attack being the detection of the existence of this covert communication.
3) Watermarking has an additional requirement with regard to its robustness against possible attacks so that even if the existence of the hidden information is known, it should be hard for an attacker to destroy the watermark (Steganography being mainly concerned with the non-detection of hidden data while watermarking is concerned with potential removal by an attack).
4) Steganographic communications are usually point-to-point (between sender and receiver) while watermarking techniques are usually one-to-many and while Steganography is primarily concerned with the capacity of hidden information and its impact on perception, watermarking can focus on the robustness of relatively small amounts of hidden data compared to the size and resolution of the host.

B. Principal Components of Digital Watermarking

All watermarking schemes share the same generic building blocks, namely, watermark embedding and information extraction [5].

Manuscript received on 1 August, 2013; and revised 20 November, 2013. This work was supported by the Science Foundation Ireland and by the Erasmus Mundus EWENT Programme, Warsaw University of Technology, Poland.

Jonathan Blackledge is the SFI Stokes Professor, School of Electrical and Electronic Engineering, Dublin Institute of Technology, Ireland. Email:jonathan.blackledge@dit.ie

Oleksandr Iakovenko is Assistant Professor, Department of Computer Science, Odessa National Polytechnic University, Odessa, Ukraine. Email:iakovenko.oleksandr@gmail.com

1) Watermark Embedding (Signature Casting): The embedded data is the watermark that one wishes to embed. It is usually hidden in data referred to as a 'cover' to produce the 'watermarked cover'. The inputs to the embedding system are the watermark, the cover and an optional key (which may include system parameters). The key is used to control the embedding process so as to restrict detection and/or recovery of the embedded data to parties who know of it. The watermarked cover may face some intentional and/or unintentional distortion that may affect the existence of the watermark.

2) Watermark Detection System (Extraction): The inputs to the detection system are the possibly distorted watermarked cover, the key and depending on the method, the original cover or the original watermark. Its output is either the recovered watermark or some kind of confidence measure indicating how likely it is for a given watermark at the input to be present in the data under inspection. Many current watermarking schemes may be viewed as spread-spectrum communication systems whose aim is to send the watermark between two parties with two sources of noise:

- noise due to the original cover;
- noise due to processing.

C. Fragility and Robustness of Watermarked Images

One of the most important issues in modern image watermarking development concerns the issue of robustness. In general, image watermarking methods fall into two basic categories:

- fragile watermarks;
- robust watermarks.

Fragile watermarks can be destroyed as soon as the image is modified in some way. They are usually applied to detect modifications of the watermarked data rather than conveying unreadable information. Compared to cryptographic techniques in regard to data authentication, there are two significant benefits that arise from using a watermark:

- the signature becomes embedded in the message;
- it is possible to create 'soft authentication' algorithms that offer a multi-valued measure that accounts for different unintentional transformations that the data may have suffered instead of a binary True/False answer given by cryptography-based authentication.

Robust watermarks have the property that it is not feasible to remove them or make them useless without destroying the image at the same time. This usually means that the mark should be embedded in the most robustly significant components of the object. It also means that the hidden information, or at least a significant portion of it, can be recovered subject to distortion from geometric features, noise and blur etc. that occur when the image is printed and scanned, for example, or when it is transmitted in a noisy environment and/or compressed for archiving.

With regard to the generic robustness of a watermarked image, the principal goal is to prevent attacks designed to diminish or remove the presence of a watermark from its associated content while preserving the content so that it is not made redundant after an attack has taken place. Important examples of 'robustness to attacks' are as follows:

1) Additive Noise: This may happen (unintentionally) in certain applications such as D/A (printing) and A/D (scanning) converters or from transmission errors. It can also happen intentionally by an attacker who is trying to destroy the watermark (or make it undetectable) by adding noise to the watermarked cover.

2) Filtering: Linear filtering such as low-pass filtering (e.g. a Gaussian Blur) or non-linear filtering such as median filtering.

3) Collusion Attack: In some watermarking schemes, if an image has been watermarked many times using different keys, it is possible to collect many such copies and 'average' them into a composite image that closely resembles the original image and does not contain any useful watermarking data [6].

4) Inversion Attack (Elimination Attack): An attacker may try to estimate the watermark and then remove it by subtracting the estimate or reverse the insertion process to remove the watermark. This means that an attacked image can not be considered to contain a watermark at all (even using a more sophisticated detector). Note, that with different watermarked objects, it is possible to improve the estimate of the watermark by simple averaging.

5) Lossy Compression: This is generally an unintentional attack which often appears in multimedia applications. Nearly all digital images that are currently distributed via the Internet are in compressed form. Lossy image compression algorithms are designed to disregard redundant perceptually-insignificant information in the coding process. Watermarking tries to add invisible information to the image in such a way that it is not perceptually significant. An optimal image coder will therefore simply remove any embedded watermark information. However, even state-of-the-art image coding such as JPEG 2000++ does not achieve optimal coding performance and therefore there is a 'distortion gap' that can be exploited for watermarking.

D. About this Paper

A commonly used image watermarking method is based on the replacement of the Least Significant Bits (LSB) in data samples of host images with bits of hidden data. However, this approach is not applicable with common multimedia file formats as modern compression techniques can severely distort the LSB during the compression process. Common examples are JPEG and MPEG formats which store multimedia information in the form of rounded (nearest integer) spectral components using the (Discrete) Cosine Transform. Quantisation in the spectral domain distorts data in the spatial domain. This leads to the near complete elimination of the LSB embedded data during compression operations. However, while LSB embedding can not be applied in the spatial domain, it can still be applied in spectral domain. Thus, the Discrete Cosine Transform (DCT) coefficients of a JPEG image can be the subject of LSB based watermarking.

In this paper we address a method that uses a spectral embedding pattern approach on a block-by-block basis. The focus of the method is on the generation of very high resilience full colour image watermarking that can be used on a print-scan basis or an e-display-scan basis for applications that include e-tickets in which QR codes are embedded

in an image of the ticket holders portrait, for example. After providing a brief overview of watermarking techniques given in Section II, we consider a new block based DCT approach and present details of its performance to various attacks associated with low resolution scans of an image watermarked using the algorithms developed. This is the subject of Section III (the DCT based algorithm) and Section IV (evaluation of the algorithm) in which the limitations associated with the DCT-based algorithm are also studied.

The limitations of the DCT lead to the study of another block based method in which the DCT is replaced with a frequency modulated wavelet or 'Chirp coding' technique which improves the robustness of the algorithms further (particularly with regard to additive noise) by virtue of the fact that the data is embedded using a phase only spectrum. This is the subject of Section V.

In order to exploit either approach (i.e. the DCT or Chirp coding method) for the development of a practically viable e-display/e-scan authentication system, it is necessary to consider algorithms for the automatic alignment of the scanned image including compensating for (partial) rotation, scale and shift, perspective and wide-angle distortion. All of these effects can occur when a digital image is acquired through a hand-held digital camera and can lead to significant errors being generated in the watermark extraction process. In this paper, new algorithms are proposed to solve these problems as given in Section VI with an experimental evaluation being provided in Section VII.

The originality of the work reported in this paper relates primarily to the algorithms associated with DCT and Chirp-coding based embedding techniques used, to the extraction processes applied, and, to the new self-alignment algorithms based on the watermark itself. The approach taken provides a set of procedures that can yield a fully automated system for high resilience watermarking with a range of practical applications.

II. Overview of Image Watermarking Techniques

Image watermarking algorithms fall into two fundamental categories:

- spatial techniques;
- transform techniques.

Spatial techniques embed information by direct data modification. They are usually simple to implement, require low computational cost but tend to be less robust.

Transform techniques encoded information by modifying the coefficients obtained from a discrete transformation using transforms such as the Fourier Transform, Cosine Transform, Wavelet Transform, Walsh Transform, Wigner Transform, Affine Transform and others.

In principle, there is no effective limit to the type and/or number of transforms that can be applied if a valuable and computationally cost effective algorithm can be designed that is functional within the constraints placed on the operational characteristics of the watermarking application under consideration. This is why there is, as yet, no provable unique watermarking algorithm that is optimal with regard to all constraints and, in turn, why so many algorithms have been considered in the literature as detailed in [1] and references therein. On the other hand, there are a large number of methods that can be strictly or loosely classified within the context of the Wavelet Transform, the difference being related to the exact wavelet that is applied.

A. Basic Theoretical Principles

If $I_{i,j}$ denotes a digital image, then a transform $\hat{T}$ is applied to yield a matrix of coefficients $c_{i,j}$

$$c_{i,j} = \hat{T}[I_{i,j}]$$

These coefficients are then modified in some way (e.g. by the replacement of selected elements with new values relating to the watermark information) thereby generating a new matrix $C_{i,j}$ such that

$$J_{i,j} = \hat{T}^{-1}[C_{i,j}] \sim J_{i,j}$$

where $\hat{T}^{-1}$ denotes the inverse operator. This process relies on both the existence and the computational stability of the transform $\hat{T}$ and its inverse $\hat{T}^{-1}$ and can be applied either to the image in its entirety on a block-by-block basis where the size of each block is an integer fraction of the image size thereby providing a greater degree of freedom with regard to the embedding of information in an image. It can also be applied to the individual channels associated with the colour model applied to a colour image thereby providing a further degree of 'colour embedding space'. In most cases, the embedded information can be of an encrypted form although this can place certain constraints on the watermarking scheme with regard to the need to decrypt the information subject to distortions due to an attack on the host image and/or watermark data, e.g. [7], [8] and [9].

Although, as mentioned before, the proliferation of watermarking schemes is a due to a lack of uniqueness criteria in respect of the transform $\hat{T}$ that is used, certain transforms are based on 'optically significant' kernels that are related to the field of mathematical modelling and computational physics [10]. For example, Fresnel optics is based on a unique quadratic phase factor in which the Point Spread Function has the form $\exp[i\pi(x^2+y^2)/f\lambda]$ where f is the focal length and λ is the wavelength associated with the 'imaging system' [11]. The same quadratic form occurs in the field of statistical mechanics, for example, yielding wavelets such as the 'Heatlet' with bi-orthogonal scaling polynomial properties [12] and in quantum mechanics in which the fundamental solution to the one-dimensional Schrödinger equation is determined by a 'Chirplet' of the form (using 'natural units') $\exp(ix^2/2t)/\sqrt{2\pi it}$ [13]. The application of a tensor product of such Chirplets to provide a set of four two-dimensional Chirplets yields very high resilience to noise using a block watermarking scheme [14]. This approach will be discussed later on in this paper.

Image watermarking methods have also been developed which make use of the non-deterministic wavelets and use a process known as 'Stochastic Diffusion' which has the advantage of encrypting the watermark by default [15] and can be applied to full colour image watermarking using three host images [16]. In this case, the transform $\hat{T}$ is based on a convolution operation with the watermark and the inverse transform $\hat{T}^{-1}$ on a correlation. Thus, if $W_{i,j}$ denotes the 'watermark image' then

$$J_{i,j} = \hat{T}[W_{i,j}] + rI_{i,j}$$

where r is the 'Image-to-Watermark Ratio' and where both arrays are taken to be positive, real and normalised. The transform can be based on the application of any Point Spread Function (stochastic or otherwise) that is a phase only function since in Fourier space (using the convolution theorem and using $\widetilde{\ }$ to denote the Discrete Fourier transform DFT)

$$\widetilde{J}_{i,j} = \exp[-z\theta(i,j)]\widetilde{W}_{i,j} + r\widetilde{I}_{i,j}$$

where $z \equiv 0 + \sqrt{-1}$ and $\theta(i,j)$ is the phase spectrum, recovery of the watermark being based on the result

$$\widetilde{W}(i,j) = \exp[z\theta(i,j)][\widetilde{J}_{i,j} - r\widetilde{I}_{i,j}] \sim \exp[z\theta(i,j)]\widetilde{J}_{i,j}$$

given that $\hat{T}^{-1}I(i,j) \sim 0$. This approach can be used to embed a significant amount of image information content suitable for image self-authentication, for example, or on a block-by-block basis to embed less information but with greater resilience to an attack. In view of this approach, the method reported in this paper uses the DCT rather than the discrete Fourier transform. While the DCT does not provide the same phase only function option for watermarking an image (because the output of the DCT is real only) it does provide similar options within the context of 'frequency space modification' in a way that is compatible with standard image compression methods.

B. Block Embedding Based Methods

One of the principal methods for developing robust, as opposed to fragile watermarking algorithms, is to apply a block embedding technique. This is because pixel-by-pixel embedding can be affected by virtually any digital and optical image distortion. To overcome this problem some regions (blocks) of an image should be used for embedding watermark 'symbols' which, in practice, are numerical values (binary, integer or both) that code the information to be embedded. The idea of block embedding lies in splitting the image into a number of blocks, and embedding hidden text symbols into each block separately. The blocks may, in principle, be irregular, but block regularity is the norm. To extract the watermark from the image, it is processed and analysed block-wise. Each block of the image can have a limited number of permitted states and during application of the watermark extraction process, each block is analysed with regard to its proximity to a defined state, the most likely state then being accepted as one of the extracted symbols as illustrated in Figure 1.

Block embedding can yield a high level of robustness and can cope with a modification to **any** pixel in an image block as well as with some types of distortion or 'attacks' that are common to optical image transmission. These include the following:

- image re-sampling and blur (typically a Gaussian blur);
- barrel/pincushion and perspective distortion;
- tone curve modification.

These properties allow us to consider not only digital image distortion but also natural optical image deformation. The watermark, which is robust to these deformations, can then be transmitted as an embedded code in the host image through an optical channel. However, in order to enhance the resilience of a watermark to the above, the quantity of information that can be used in the watermark is reduced. A number of diverse block transform modification techniques can be developed but in this paper we focus on DCT coefficient modification and Chirplet block coding which can be viewed in terms of a pattern addition process.

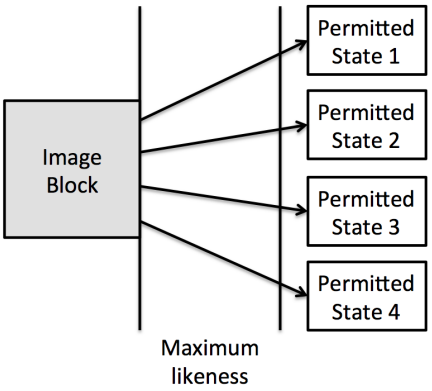

Fig. 1. During the extraction of a watermark, each image block is analysed with regard to its proximity to four permitted states. The maximum likeness criterion is used to determine the 'closest' state.

III. DCT Coefficient Embedding Algorithms

The DCT produces a set of real coefficients that, on a block-by-block basis can be modified to embed the watermark data. In this section, we provide an overview of the algorithm developed for this purpose. The algorithm has been designed with a specific focus on optimising performance in terms of robustness to e-display-to-scan distortions where the (watermarked) image is captured using a low resolution mobile phone camera, for example. Compared to the application of the DCT for e-to-e watermarking scheme, this requires that the watermark is particularly robust to distortions of noise and blur which are discussed later in the paper. The algorithm developed assumes, by default, the use of full 24-bit colour images which provides greater 'colour space' for the watermarking procedure than a grey level image and is used as part of the embedding process.

A. Outline of the DCT-based Watermark Embedding Algorithm

1) The host or container image I_c is converted from RGB to YCbCr colour mode. Only colour channels C_b and C_r are modified during the embedding processes. This is because embedding in a brightness channel is more noticeable thereby requiring smaller amplitudes of perturbations.
2) Each colour channel is split into number of regular blocks of pixels B_k^B (blue) and B_k^R (Red), $k = 1, 2, ..., L$, each block being taken to be a matrix of pixel values:

$$B = [b_{i,j}], i = 1, 2, ..., M, j = 1, 2, ..., N$$

The dimensions of each block (M and N) are chosen to keep the block shape as close to a square as possible.
3) The embedding data h is protected with an error correction code, resulting in data extension:

$$\mathbf{h}'_t,\ t = 1, 2, ..., 2L$$

4) The two-dimensional Discrete Cosine Transform (DCT) is performed on each block:

$$X_{m,n} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} b_{i,j} \cos\left[\frac{\pi}{M}\left(i+\frac{1}{2}\right)m\right] \cos\left[\frac{\pi}{N}\left(j+\frac{1}{2}\right)m\right],$$

where $X_{m,n}$ are the DCT spectrum components of block B_k, $m = 1, 2, ..., M, n = 1, 2, ..., N$.

5) DCT components of a block are then modified according to one of a number of possible patterns and, for simplicity, the system design for two embedding patterns P_0 and P_1 is described. Each pattern replaces some of the DCT components with exact values and represents one bit of the embedded data $\mathbf{h}'_t$. For example:

$$P_0 : [X_{4,6} = 0, X_{6,4} = -A, X_{10,8} = 0, X_{8,10} = A]$$
$$P_1 : [X_{4,6} = A, X_{6,4} = 0, X_{10,8} = -A, X_{8,10} = 0],$$

where A is the amplitude of the spectral perturbation whose specific value affects the watermark visibility and system robustness characteristics. The choice of the exact embedding patterns has great significance on the robustness and visibility of the watermark. The patterns are chosen in a way that makes the system robust to carrier image modification which is addressed later on in this paper.

6) The two-dimensional Inverse Discrete Cosine Transform (IDCT) is performed on the perturbed spectrum $X'_{m,n}$:

$$B' = \left[b'_{i,j}\right] = \text{IDCT}\left(X'_{m,n}\right)$$

7) The modified blocks B'_k are concatenated in the same manner as in the initial image forming new colour channels C'_b and C'_r and these (modified) channels combined with the intact lightness channel to produce the resulting watermarked image I'_c which is converted back to RGB colour space.

8) The watermarked image is saved in one of a number of image storage formats, being insensitive to image compression settings with the exception of *lowest quality* compression in lossy formats, such as JPEG. The watermarked image can then be printed or displayed on a monitor for application of the extraction process which is described in the following section.

B. Outline of the Watermark Extraction Algorithm

1) The watermarked image I'_c, displayed on a monitor or printed on paper, is captured on a digital camera where the average phone camera quality is taken to be generally sufficient for extraction, the critical capturing distance and orientation depending on a number of parameters, including the embedding amplitude A, embedding patterns P, image size and number of blocks L.

2) The image is aligned and cropped by any accessible means to match the original image as discussed in Section III (A).

3) Conversion to YCbCr colour mode is performed with only the colour channels C_b and C_r being analysed.

4) Each channel is split into blocks B_k as used in the embedding procedure discussed in the Section III (A).

5) The Discrete Cosine Transform is performed for each block:

$$\mathrm{X} = [X_{m,n}] = \text{DCT}\left(\mathrm{B}_k\right)$$

6) The spectrum of each block is then evaluated to detect the presence of each pattern. The most likely identifying pattern in each block yields one bit of the embedded data and for the embedding patterns discussed in Section III (A), each embedded bit is determined by:

$$\mathbf{h}'_t = \begin{cases} 0 & \text{if } (X_{8,10} - X_{6,4}) > (X_{4,6} - X_{10,8}), \\ 1 & \text{otherwise.} \end{cases}$$

7) The Recovered data $\mathbf{h}$ is then obtained from $\mathbf{h}'$, using an error correction code.

In the following section, the principal results associated with a series of optical and numerical experiments are provided that yield a quantitative assessment of the algorithms in terms of the resilience of the watermark data to a range of attacks.

IV. Evaluation of the DCT Embedding Algorithm

We consider a container image I_c shown in Figure 2 which is a full 24-bit colour image and has a size of 500×500 pixels and where its colour channels C_b and C_r are split into $k = 11 \times 12 = 132$ blocks each. The size of each block B_k is 40×44 pixels. This particular image is chosen as a test case because of its relative homogeneity and object-to-background clarity thereby providing a quality control measure in terms of the visual impact of a watermark that is not prevalent with more complex and textured container images. Figure 2 also shows a typical example of a screen shot obtained using a mobile phone camera for the watermarked image displayed on an LCD exhibiting Moire fringes.

Fig. 2. Container image used for evaluation of the DCT embedding algorithms (left) and an example of a watermarked image obtained from an LCD screen using a mobile phone camera (right).

The embedding data $\mathbf{h}$ consists of 71 bits and after application of error-correcting code BCH(255,71) the length of coded data is 255 bits [17]. This code is capable of correcting up to 30 bit errors and more up-to-date codes such as LDPC can be used to boost system efficiency. Taking each block to carry one bit, the total number of available embedding bits is $2L = 264$. However, since $264 - 255 = 9$, there are nine extra blocks in the lower right hand corner of the image which are not affected by the watermarking procedure, five of these blocks belonging to C_b and four to

the C_r channel. On this basis, we consider the resilience of the algorithms presented in Section 3.1.1 and Section 3.1.2 to the 'attacks' discussed in the following sections.

A. Robustness to Additive Noise

As long as the system uses Forward Error Correction, the Bit Error Rate is not an optimal parameter for performance evaluation. The system is designed to be bit-error free and so an evaluation is focused on a relationship which connects error robustness with watermark intensity, given that the watermark is extracted properly. The robustness of the system to noise is highly dependent on the embedding rate R which relates the spectral perturbation intensity to the original spectrum intensity. The noise intensity is expressed in terms of the percentage of image intensity with measurements being performed in the following manner: (i) the embedding rate R is fixed; (ii) the noise intensity is raised until error correction fails; (iii) the most intensive noise, allowing error-less extraction, is taken as a 'reference marker'. The result is shown in Figure 3 which includes an example of the most intensive case of additive Gaussian noise that does not affect the watermark data.

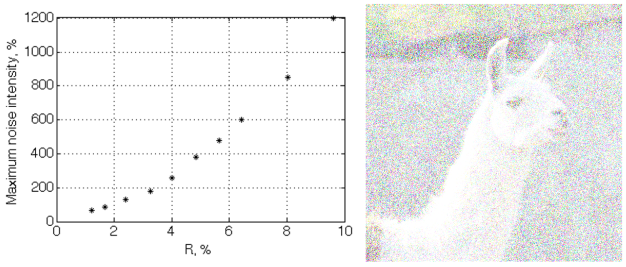

Fig. 3. Watermark noise robustness for different embedding rates R (left) and an example of a high noise rate corresponding to a case which does not affect the watermark data.

B. Robustness to a Gaussian Blur

Robustness to image blurring depends on the particular set of DCT-coefficients that are used in the embedding patterns. If the radius of a Gaussian blur, for example, is less than the scale of embedded detail, then the blur does not distort the watermark providing extraction is good. However, when the radius is equal or larger than the scale of embedded detail this detail is dissipated in the blur and extraction becomes impossible. A Gaussian blur with a pixel radius up to and including 12 allows for proper watermark extraction but beyond this threshold the blur erases the watermark. However, this effect does not depend on the embedding rate R.

C. Robustness to Image Shift

Shift robustness also depends on the specific embedding coefficients. However, if the embedding patterns use the same set of embedding frequencies (which is optimal for noise robustness) then the spatial pattern P^s appears similar to it's counter-pattern shifted in some direction as illustrated in Figure 4. While a 3 pixel shift is easily recovered, a 4 pixel shift, either vertically of horizontally, prevents successful watermark recovery, regardless of the embedding rate.

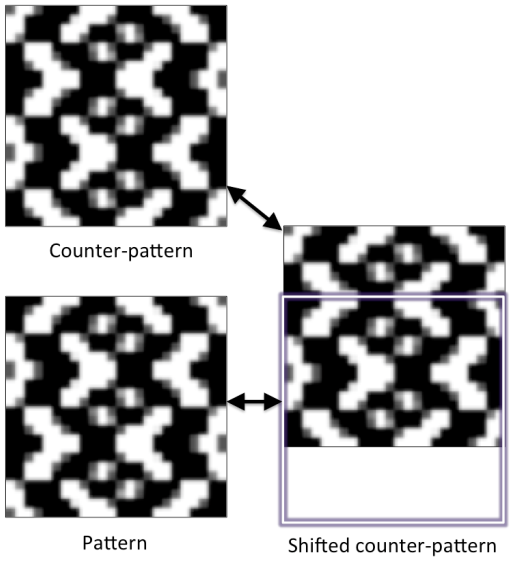

Fig. 4. Illustration of a shifted pattern which can be erroneously recovered as a counter-pattern.

D. Robustness to 'Barrel' and Rotational Distortions

Geometric image distortions such as barrel, pincushion and rotational distortions are tightly connected with image re-sampling and optical image deformation. These distortions need to be corrected in an image alignment procedure and the results discussed in this section are devoted to illustrating the systems reaction to improper alignment. Watermark recovery is not disrupted by re-sampling and a major problem with barrel/rotation distortions is the displacement of edge embedding blocks which appear shifted with regard to the recovery procedure. Neither barrel or rotational distortions depend upon the embedding rate R and a marginal barrel parameter such as $3.0 \cdot 10^{-5}$ and a rotation of less than $\pm 0.85^{\circ}$ does not affect accurate watermark extraction. However, these results depend significantly upon the container image and embedding block sizes.

E. Robustness to Partial Removal of Image Data

The partial removal of an entire section of the watermarked image will clearly lead to complete corruption of the watermark data in the same section. However, it is important to evaluated the effect of this on watermark extraction over the rest of the image. Figure 5 clearly illustrates that the effect of removing data from a portion of the image (in this example, the lower left-hand corner of the image) does not affect the remaining portion of the image with regard to watermark extraction whose performance characteristics are the same with regard to the robustness criteria discussed in the previous sections.

F. DCT-embedding applicability considerations

The DCT coefficient embedding algorithm presented in this paper depends (as with all algorithms) on the specific embedding pattern used and other algorithmic parameters. However, in the context of the focus on using a DCT based approach to produce a highly resilient watermarking method, we may conclude with some common conceptual

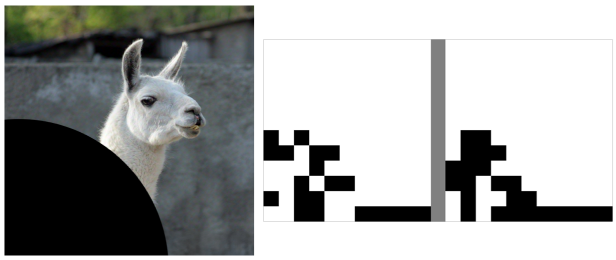

Fig. 5. Example of the bit-errors generated in both channels (right) by the partial removal of a portion of the watermarked image (left). The rest of the image on the right-hand-side is white indicating that there are no bit-errors in the remaining portion of the watermark after extraction from the spoiled image. Note that error correction coped with such a data modification, and watermark was extracted error-less.

strengths and weaknesses. The strengths/weaknesses listed below are primarily concerned with the watermark robustness characteristics and do not relate to watermark capacity or visibility factors.

1) Strengths:

1) Robustness to additive noise (with a proper set of embedded patterns) and robustness to image re-sampling.
2) Flexible visibility and robustness characteristics through choice of different patterns and robustness to scaling (within certain limits).

2) Weaknesses:

1) Sensitivity to image shifting.
2) Sensitive to image blur (especially if the patterns include high-frequency coefficients).

The sensitivity to shift is one of the principal problems associated with application of the DCT in general. Though patterns can be isolated that have different spatial frequencies, noise robustness requires that a counter-pattern should be as close as possible to an intensity-inverted initial pattern. But due to the periodic nature of DCT-component patterns, shifted patterns can be easily recovered as counter-patterns - see Figure 4. However, subject to the weakness listed above, the algorithm presented in this paper does provide a DCT based watermarking method that is practically applicable to print/e-display-to-e-scan detection that is inclusive of (marker-independent) automatic alignment. To the best of the authors knowledge, this is the first DCT-based algorithm of its type that can be used in this way.

V. Chirplet Based Watermarking

In this section, we report on the use of two-dimensional *Chirplets* for embedding binary data in digital images, which, to the best of the author's knowledge, represents another original contribution to the field. After briefly reviewing what chirplets are and the combinations available we study their optimisation with regard to Bit-Error-Rates. On the basis of this study, new watermark embedding and extraction algorithms are presented with a focus on the robustness of the approach to image distortion.

A. Chirplet pattern watermarking

The applications of digital watermarking and information hiding are well known and involve numerous approaches based on both direct data modification (e.g. Least Significant Bit embedding) and transformation based modification using the Discrete Cosine and Wavelet transforms, for example. Methods of encoding the hidden information are also diverse and range from bit-for-bit encryption schemes to the use of Stochastic Diffusion [18]-[19]. With regard to bit stream encoding for embedding information in digital signals, 'Chirp Coding' [20]-[21] is the one of the most robust techniques with regard to distortion through additive noise. While this technique has been successfully applied to audio signal authentication and self-authentication problems [22] for Digital Rights Management in the audio post-production industry, its potential to image watermarking applications is not yet explored. Image watermarking systems were offered, using full-image chirplet parameters embedding [23]-[24].

B. Chirplet Combinations

Chirplets can be defined in a number of related but strictly different forms, and, by combining these forms, different chirp coding methods can be developed. This is a central theme of the work reported here, and, in the following sections, we introduced the one-dimensional and two-dimensional chirplet combinations that are available.

C. One-dimensional Chirplets

One-dimensional chirps are swept-frequency co-sinusoidal signals. In a linear chirp, for example, the frequency f of oscillation is a linear function of time t, i.e. $f(t) = f_0 + kt$ where f_0 is the carrier frequency and k is a constant that define the extent of the chirp - the 'Chirping Parameter'. 'Chirplets' are time limited chirps or chirps of compact support characterised by a frequency range that sweeps from some minimum to some maximum value or vice versa.

In the time domain, a real chirplet can be defined as (for some arbitrary constant θ_0)

$$x(t; f_0, k, \theta_0) = \begin{cases} \sin \\ \cos \end{cases} \left[2\pi \left(f_0 t + \frac{k}{2} t^2 + \theta_0 \right) \right]$$

or in complex form, as

$$x(t; \omega_0, \alpha, \beta) = \exp[i(\omega_0 t + \alpha t^2 + \beta)]$$

where ω is the angular frequency, $\alpha = \pi k$ and $\beta = 2\pi\theta_0$

D. Two-dimensional Chirplets

One-dimensional chirplets can be combined to produce two-dimensional chirplets on a row/column by row/column basis to produce a matrix of essentially one-dimensional chirplets. However, for applications to non-separable image processing, it is preferable to use two-dimensional patterns instead. This approach yields some significant advantages in the robustness of chirplet watermarking which is a focus of the work presented in this paper as discussed later.

Since the application of the technique focuses on digital images, chirplets are used in discrete form in which they appear as vectors of size N composed of consecutive stream of uniformly sampled real floating point numbers between -1 and $+1$ inclusively, i.e.

$$\mathbf{c} \equiv \mathbf{c}_i \in [-1, 1] \forall i = 1, 2, ..., N$$

We consider a $N \times N$ matrix P formed from the dyadic tensor product of the vector $\mathbf{c}$ to produce a two-dimensional chirplet as given by the equation

$$P = \mathbf{c}^{\mathbf{T}}\mathbf{c} \equiv \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix} \begin{pmatrix} c_1 & c_2 & \dots & c_N \end{pmatrix}$$

$$= \begin{pmatrix} c_1c_1 & c_1c_2 & \dots & c_1c_N \\ c_2c_1 & c_2c_2 & \dots & c_2c_N \\ \vdots & \vdots & \ddots & \vdots \\ c_Nc_1 & c_Nc_2 & \dots & c_Nc_N \end{pmatrix}$$

However, the chirplet vectors elements used to construct equation P can be constructed in both a 'forward' and 'reverse' order. This produces a total of four distinct two-dimensional chirplet patterns as given below:

$$P_1 = \mathbf{c}^{\mathbf{T}}\mathbf{c} \quad (1)$$

$$P_2 = \text{reverse}(\mathbf{c})^{\mathbf{T}}\mathbf{c} \quad (2)$$

$$P_3 = \mathbf{c}^{\mathbf{T}}\text{reverse}(\mathbf{c}) \quad (3)$$

$$P_4 = \text{reverse}(\mathbf{c})^{\mathbf{T}}\text{reverse}(\mathbf{c}) \quad (4)$$

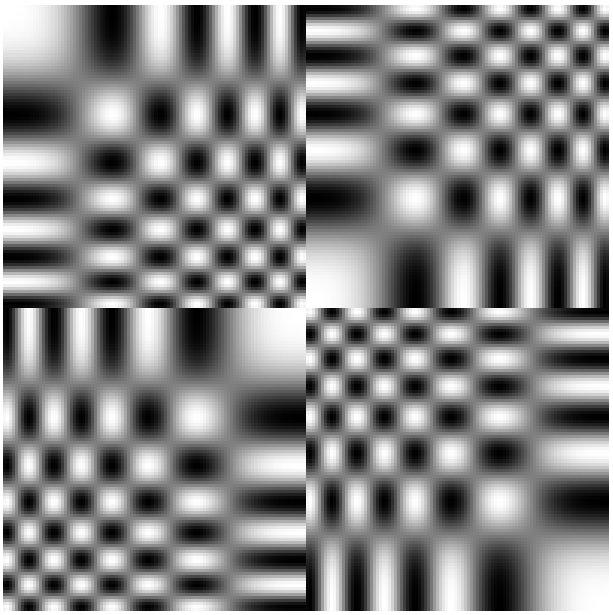

Fig. 6. Four distinct two-dimensional chirplet patterns associated with equations (1)-(4) (clockwise, respectively).

The operation 'reverse' denotes the reversal of the order of the elements in the vector $\mathbf{c}$ used to construct the matrix P, i.e. if

$$\text{reverse}(\mathbf{c} = \{c_1, c_2, ..., c_{N-1}, c_N\}) = \{c_N, c_{N-1}, ..., c_2, c_1\}$$

The patterns produced by these two-dimensional chirplets as given by equations (1)-(4) as illustrated graphically in Figure 6. Each of these patterns can be used to assign two bits of information and as there are four possible embedding patterns it is possible to encode the four fundamental binary pairs 00, 11, 01 and 10.

E. Optimal Chirplet Combinations and Parameters

For information hiding applications, a set of embedding patterns is defined to represent different symbols associated with the embedded data. For binary information hiding, the patterns, corresponding to 0 and 1, should be as separable as possible in order to maximise the robustness of the watermarked host image subject to a range of distortions and perturbations. The embedding patterns for 0 and 1 should be *different* in some way. For a chirplet signal, the term *different* can be ambiguous. Thus, if a chirplet $\mathbf{c}$ is considered to be **forward**, the **reverse** chirplet is obtained by:

- *Value Inversion*: $-\mathbf{c}$;
- *Time reversal*: reverse$(\mathbf{c})$;
- *Time Reversal and Value Inversion*: $-$reverse$(\mathbf{c})$;

F. Optimal Chirplet Type Combinations: Robustness to Noise

To illustrate the principle of optimal chirplet combinations, we choose *noise robustness* as a criterion for chirplet separability for the one-dimensional case. A stream of 3000 random bits $\mathbf{r}$ (i.e. a stream of 1's and 0's) is generated and three sequences of chirplet signals generated, one sequence corresponding to each of the chirplet pairs described above. Thus we generate the signal

$$\mathbf{s} = \mathop{\Big\|}_{i=1}^{3000} \mathbf{c}_i \equiv \mathbf{c}_1 \,\|\, \mathbf{c}_2 \,\|\, \cdots \,\|\, \mathbf{c}_{3000}$$

where

$$\mathbf{c}_i = \begin{cases} \mathbf{c}_{\text{forward}} & \text{if } \mathbf{r}_i = 1 \\ \mathbf{c}_{\text{reverse}} & \text{otherwise} \end{cases}$$

and $\|$ denotes concatenation of the vectors $\mathbf{c}_i$

Gaussian noise $\mathbf{n}$ is then added to each sequence where the Noise-to-Signal Ratio (NSR) (the 'Noise Intensity') is taken to be a multiple of the chirplet amplitude. Thus we generate the 'noisy signal'

$$\mathbf{s}_n = \mathbf{s} + \text{NSR}\mathbf{n}$$

the problem now being to recover or 'detect' the bit stream, 'chirp coded' in the vector $\mathbf{s}$. The detection is performed through *cross-correlation* of the vector $\mathbf{s}_n$ with two chirplets:

$$\mathbf{d}_1 = \mathbf{s}_n \star \mathbf{c}_{\text{forward}}$$

$$\mathbf{d}_2 = \mathbf{s}_n \star \mathbf{c}_{\text{reverse}}$$

where $\star$ denotes the correlation sum. The correlation maximums are then evaluated to detect each bit in the output stream and by dividing the number of erroneous bits by 3000, the 'Bit-Error-Rate' (BER) is computed. The computation is repeated with different noise intensities which yield the results shown in Figure 7 The results show that among the chirplet pairs possible, the pair with *Time Reversal* (the Red Signal given in Figure 7) shows considerably lower BERs for different noise intensities compared to the other chirplet pairs used. The results is effectively the same for different chirplet parameters (e.g. the 'Chirping Parameter'). Thus, in the application of 'Chirp Coding' for hiding binary data in digital signals (e.g. [20], [25] and [21]), *Time Reversed Chirplet Pairs* provide optimal performance. We now discuss the issue of optimising the chirplet parameters.

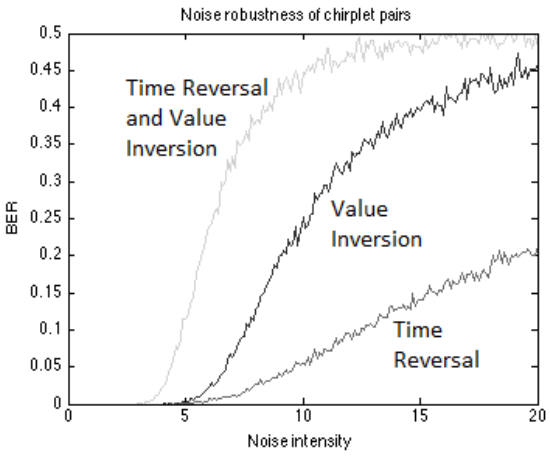

Fig. 7. Bit-Error-Rate (BER) as a function of the Noise Intensity (Noise-to-Signal Ratio) for three different chirplet pairs as indicated, namely, Time Reversal and Value Inversion, Value Inversion and Time Reversal.

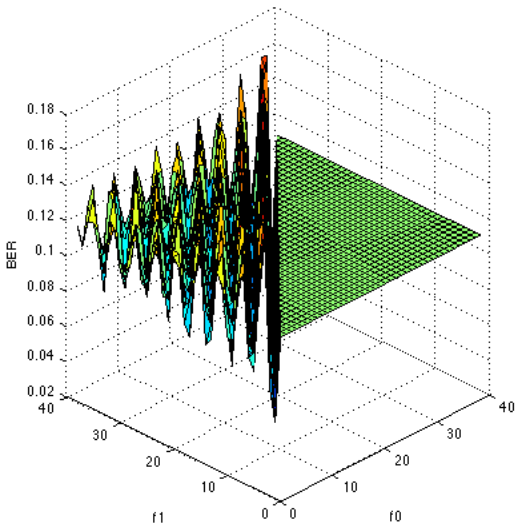

Fig. 8. Bit-Error-Rate (BER) as a function of f_0 and $f_1 > f_0$ for Time Reversed Chirplet Pairs.

G. Optimal Chirplet Parameters

Chirplets are signals which have following fundamental parameters:

- Starting Frequency f_0;
- Terminating Frequency f_1;
- Type of frequency sweep: Linear, Quadric, Logarithmic, etc.

Given the set of target characteristics, some particular chirplets can be considered optimal. Numerical experiments were therefore conducted to define the optimum combination of $\min f_0$ and $\max f_1$ for a linearly frequency swept chirplet in terms of achieving maximum robustness to additive Gaussian noise with a Noise Intensity set to 20. For each combination of f_0 and $f_1 > f_0$, the value of the BER was computed using 2000 chirplet samples in a sequence using *Time Reversed Chirplet Pairs*. The resulting surface plot corresponding to the function $\mathrm{BER}(f_0, f_1)$ is shown in Figure 8.

The Figure shows that chirplet noise resiliency highly depends on chirplet starting and ending frequencies (the BER deviation is about 15%), especially on their sum $f_1 + f_0$. On the basis of this surface plot, the optimum chirplet parameters yielding optimal robustness to noise can be obtained.

Having established some important numerical issues with regard to using chirplets for signal based bit information hiding, we now consider the details associated with the principal algorithms used for watermarking (grey-level) digital images (with binary information) and assess the robustness of the approach to a range of distortions. It is noted that the same approach can be used for full 24-bit colour images by decomposing them into their RGB (or YCbCr) components, details of which lie beyond the scope of this paper.

H. Watermark Embedding Procedure

The principal steps associated with the algorithm for embedding binary data in a grey-level image is as follows:

1) Open a *Grayscale Container Image* I_c, which is taken to be normalised, i.e. $\mathrm{I}_c \in [0, 1]$ (working with images of size 500×500 pixels for 'proof of concept' only)
2) Prepare the data for embedding $\mathbf{h}$ which is composed of 25 groups, 2 bits in each group: $\mathbf{h}_k = \{b_1, b_2\}$, $k \in [1, 25]$.
3) Define the set of four chirplet patterns P_i, $i \in [1, 4]$, each chirplet being composed of 100×100 elements and where chirplet values lie in interval $[-1, 1]$.
4) Generate the *Embedding Data Array* E be grouping together 25 chirplet patterns C_k into one matrix as given by

$$\mathrm{E} = \begin{bmatrix} \mathrm{C}_1 & \mathrm{C}_2 & \mathrm{C}_3 & \mathrm{C}_4 & \mathrm{C}_5 \\ \mathrm{C}_6 & \mathrm{C}_7 & \mathrm{C}_8 & \mathrm{C}_9 & \mathrm{C}_{10} \\ \mathrm{C}_{11} & \mathrm{C}_{12} & \mathrm{C}_{13} & \mathrm{C}_{14} & \mathrm{C}_{15} \\ \mathrm{C}_{16} & \mathrm{C}_{17} & \mathrm{C}_{18} & \mathrm{C}_{19} & \mathrm{C}_{20} \\ \mathrm{C}_{21} & \mathrm{C}_{22} & \mathrm{C}_{23} & \mathrm{C}_{24} & \mathrm{C}_{25} \end{bmatrix}$$

where

$$\mathrm{C}_k = \begin{cases} \mathrm{P}_1, & \text{if } \mathbf{h}_k = \{0, 0\}; \\ \mathrm{P}_2, & \text{if } \mathbf{h}_k = \{0, 1\}; \\ \mathrm{P}_3, & \text{if } \mathbf{h}_k = \{1, 0\}; \\ \mathrm{P}_4, & \text{if } \mathbf{h}_k = \{1, 1\}; \end{cases}$$

and as shown in Figure 9. Note that the size of E is equal to the size of I_c but for arbitrary sizes of I_c, E can be zero padded.
5) The *Watermarked image* W is then acquired by addition of the *Embedding Image*, scaled with an *Embedding Rate Factor* R, to the *Container Image*, i.e.

$$\mathrm{W} = \mathrm{I}_c + R \cdot \mathrm{E}$$

By changing the value of R, it is possible to find an optimal trade-off between invisibility of the watermark and robustness with regard to watermark extraction. Typical values for R lie between 0.01 (maximum invisibility) and 0.07 (maximum robustness).

Embedding can also be accomplished with only one bit per pattern. In this case, only two from four possible two-dimensional chirplet patterns are used. The embedding capacity associated with this approach is half (i.e. 25 instead of

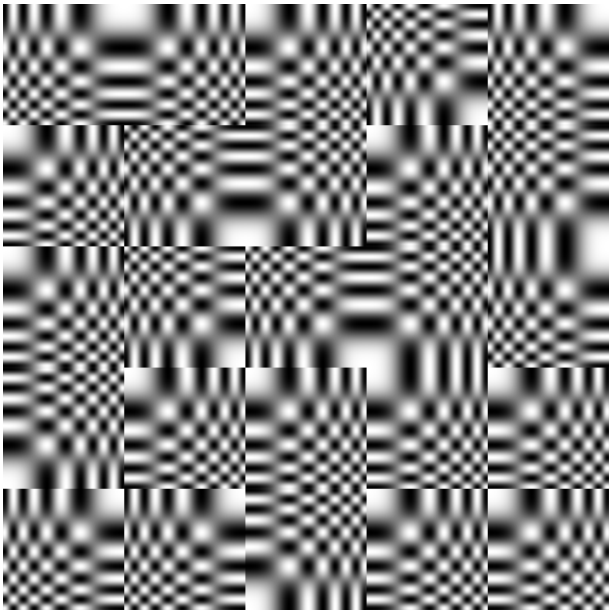

Fig. 9. Embedding map E, consisting of 25 two-dimensional chirplet patterns.

Fig. 10. Example of image with embedded watermark, $R = 0.03$.

50 bits) but it provides greater robustness and the Embedding Ratio can be set to a lower value.

I. Watermark extraction

Chirplet pattern detection is performed in the same way as the matching detection of any pattern, namely, through (two-dimensional) cross-correlation of the watermarked image with each of four embedding patterns, i.e.

$$\mathrm{D}_i = \mathrm{W} \star\star \mathrm{P}_i, \;\; i \in [1, 4] \tag{5}$$

where $\star\star$ denotes the two-dimensional cross-correlation sum. As with other matched filtering methods, if a region of the image contains an embedded chirplet pattern which matches the correlation kernel, then the central part of the cross-correlation surface has a distinct maximum showing the presence of a matching pattern as illustrated in (Figure 11). This property allows us to perform two important operations:

- Make a decision with regard to the embedded pattern based on direct comparison.
- Detect the position of the centre of the embedding block upon extraction of the watermarked channel, e.g. when the watermarked image has been subjected to shift, re-sampling and other deformations and distortions.

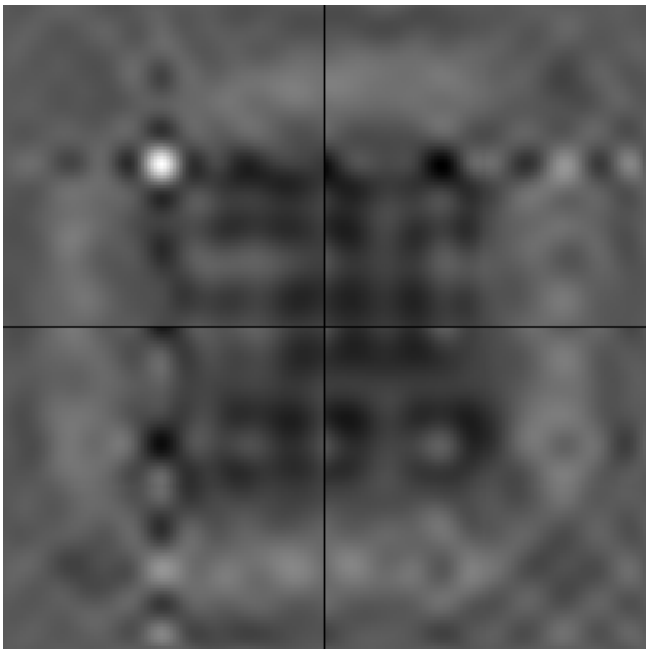

Fig. 11. Results of cross-correlating one region with four chirplet patterns. The bright spot in the centre of the top-left block indicates the presence of the first chirplet pattern in a region.

If we assume that the original block-by-block positioning is known, then the extraction procedure can be formalised using the following steps:

1) The watermarked image W undergoes a two-dimensional cross-correlation (equation 5) with each of the four embedding patterns used.
2) For each embedding region, only the central components of the correlation surface are stored. These 'central components' can be defined in a number of ways, and a detection filter can also be implemented. In this work, the central components are defined as a square 7×7 matrix extracted from the centre in each block of the correlation surface.
   Figure 12 shows these central components matrices for each of 25 embedding blocks, every central component matrix obtained from cross-correlation of block with one of four embedding patterns.
3) Compute the average value of the central component in each of the four central regions for each embedding block:
$$A_i = \mathbf{M}(\text{Central part of } \mathrm{D}_i), \;\; i \in [1, 4]$$
4) Compare the average values A_i and locate the maximum value together with its associated index i which uniquely identifies $\mathbf{h}_k$.

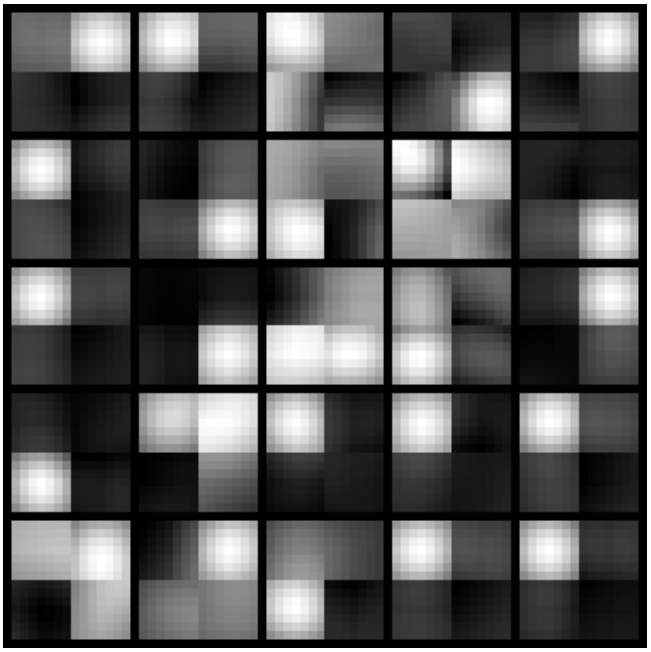

Fig. 12. The central components generated by cross-correlating each embedding region with each of four embedding patterns — see equation (5).

Given the basic steps above, we now explore the robustness of the watermarking method when the watermarked image is subjected to a range of distortions.

TABLE I
SUMMARY OF RESULTS OBTAINED THROUGH THE NUMERICAL EXPERIMENTS UNDERTAKEN TO ASSESS THE ROBUSTNESS OF THE METHOD TO IMAGE DISTORTION USING THE FIVE CATEGORIES LISTED, I.E. SHIFT, NOISE, BARREL, GAUSSIAN BLURRING AND ROTATION.

Type of Distortion	BER
No Distortion	0.06
Shift (By any Extent)	0.06
Noise (Intensity)	
5	0.06
10	0.06
20	0.06
40	0.06
80	0.04
160	0.06
320	0.10
Barrel (Distortion Intensity)	
0.5	0.12
1	0.20
Gaussian Blur (Blur Radius)	
5	0.06
10	0.08
15	0.10
20	0.16
Rotate (CCW Degrees)	
1	0.12
2	0.18

J. Robustness to distortion

To quantify the practical viability of the proposed method, a number of numerical experiments were conducted with the aim of measuring the actual watermark robustness characteristics given that the data watermarking and recovery processes are the same as in algorithms outlined in Sections V-H and V-I. This included the following basic steps:

1) Distorting the watermarked image in some way, the exact types of distortions being listed in Table I.
2) Extracting a watermark from the distorted image using the watermark extraction algorithm described in V-I.
3) Comparing the embedded and extracted data and computing the Bit-Error-Rate.

The results are compounded in Table I. In some regions of the image, hidden data is extracted with errors even when there is no distortion. The cause of this lies in the nature of the 'container image', some regions of which can contain some pronounced chirplet-like patterns themselves. However, an appropriate selection of chirplet parameters together with an adjustment of the *Embedding Rate Factor* R can diminish this effect. Any shift in the image pixels can be detected and thereby eliminated and the Noise Intensity is taken as a percentage of the image intensity.

While performing a barrel (pincushion) distortion, a new radius of each point r_n is calculated from the old radius r according to the equation $r_n = r + ar^3$, where a is the Barrel Distortion Intensity (divided by 10^6). These results are achieved without correction with regard to recovering the initial positions. However, it is noted that this correction can significantly improve robustness to these types of distortion.

VI. AUTOMATIC ALIGNMENT

Irrespective of the transformation and/or coding method used for embedding (including the DCT transform and chirp coding techniques reported in this paper), an error-less extraction of embedded data relies on proper image alignment, and, in this section we discuss a novel method for aligning the image using the same watermark data. The idea is to use the watermark to align the image before final extraction of the watermark itself.

If the container image I_c is known, an alignment procedure via the image contents can be performed. However, this approach introduces additional limitations on the watermarking system. A common solution to this problem lies in the addition of special alignment markers on the image which allow for automatic alignment. These markers can flag the fact that a watermark may be present in the image thereby initiating a potentially successful attack. For this reason, the approach described here does not rely on any additional markers. This is because the presence of embedding patterns in the image blocks' yields a DCT spectrum that, in effect, provides a set of hidden markers located at the centre of each block. This idea is compounded in the following procedure:

1) The embedding block patterns are extracted in image space starting with an empty spectrum X^0 given by

$$\mathrm{X}^0 = \left[X^0_{m,n}\right] = 0$$

The embedding pattern P is added to X^0 and the two dimensional IDCT is performed and repeated for all embedding patterns P_v, $v = 0, 1, ..., V-1$. Although the total number of patterns used in the results reported here is $V = 2$, the system can use a larger number of embedding patterns at the cost of lower robustness but increased capacity. The spatial embedding patterns

$$P^s_v = \mathrm{IDCT}(\mathrm{X}^0 + P_v)$$

are rectangular image blocks which indicate the presence of spectral patterns P_v in the block spectrum.

2) For each of the colour channels of the input watermarked image C_b and C_r, cross-correlation is performed with each of the embedding patterns P_v where, in the output $\Theta = [\theta_{x,y}]$, negative values are replaced by zeros, i.e.

$$(\theta_v)_{x,y} = \begin{cases} (C_r \star\star P_v^s)_{x,y} & \text{if } (C_r \star\star P_v^s)_{x,y} > 0, \\ 0 \text{ otherwise.} \end{cases}$$

where $\star\star$ denoted the two-dimensional cross-correlation operation. All the results for a particular colour channel are combined additively, i.e.

$$\Theta = \sum_{v=0}^{V-1} \Theta_v$$

3) The correlation results for both colour channels are also added together, i.e. $\Theta = \Theta_b + \Theta_r$. The *Characteristic Picture* Θ has the same size as the Container Image and consists of multiple cross-correlations. Each of these results have a pronounced peak in the correlation surface which locates the centre of each embedding block. A typical example of the output is shown on a Figure 13.

Using this procedure, coupled with some 'intelligent filtering' applied to Θ, the correlation peaks can be used as markers for the automatic image alignment and thus realignment of an image, realignment being undertaken through application of the Radon transform, for example [1].

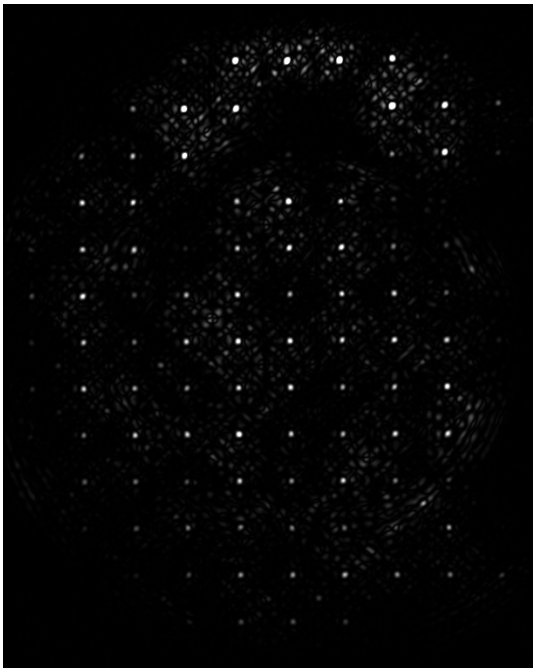

Fig. 13. Example of *Characteristic Picture* Θ generated in the correlation surface that identifies the blocks associated with the presence of the watermark data.

A. Automatic alignment

For the watermarking schemes described in this paper, error-less watermark extraction is feasible only if the watermarked image is properly aligned and divided into blocks in the same way as undertaken during the watermark embedding process. This condition holds by default if the watermarking system uses purely electronic image transmission. However, in case of optical image acquisition (which is the focus of the research reported in this paper), the image is considered to have been acquired through optical-to-digital conversion from a digital camera or (digital) scanning sensor. In this case, the image can be distorted by a number of factors which include:

- the image is rotated by some angle;
- the image is scaled (it's pixel dimensions depend on the sensor resolution and depth of focus);
- the image is generally larger than the area of interest which contains watermarked image and needs to be cropped and shifted to match the required form;
- the image often experiences noticeable amounts of perspective distortion;
- during the photographic acquisition process, the image can also be distorted by wide-angle distortions.

As mentioned previously, knowledge of the embedding pattern allows extraction of the embedding blocks' central points. This section described a new algorithm which performs automatic alignment of an acquired image based on the Characteristic Picture Θ, derived from it.

Knowledge of the container image I_c is not necessary for automatic alignment. Extraction of block centre positions relies on knowledge of the embedding patterns P_v only and it is important to note that spatial patterns should be scaled to perform superior block centres extraction.

For automatic alignment, the extraction side only requires information on the number of blocks in the image $M_b = mn$ and configuration of these blocks within the image - the number of blocks in column m and in row n. This information unambiguously defines the *Template Characteristic Picture* Θ_T which consists of $m \times n$ square blocks filled with *zero values*. In the centre of each block there is one element filled with a *maximum value* (see Figure 14).

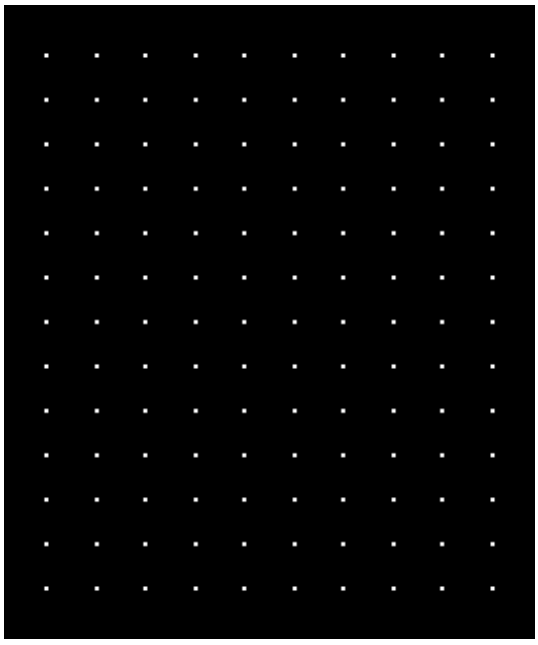

Fig. 14. Template Characteristic Picture Θ_T.

To automatically align the acquired image it must pass through a set of procedures, the parameters of these procedures being derived from the Characteristic Picture Θ. The procedures are designed in such a way as to yield a version of Θ that is 'closer' to Θ_T leading to overlapping (within a certain deviation). When the procedures are complete, the acquired image I_a undergoes the same set of procedures with the same inputs as it's characteristic picture Θ which leads to alignment of the embedding blocks to Θ_T. As the position of embedding blocks in Θ_T is known (and even controlled) the acquired image I_a can be divided into it's embedding blocks and analysed via the extraction algorithm.

The set of alignment procedures consists of:

- Image rotation compensation, which ensures that the image appears in the same angular position as it was during the embedding operation which is a key procedure and should be performed first.
- Scale and shift compensation where the image is scaled and shifted by both vertical and horizontal axes in such a way that the centres of the embedding blocks coincide with respective centres of Θ_T, the rest of I_a then being cropped.
- Perspective distortion compensation when the image experiences perspective distortions which are detected and corrected.
- Barrel/pincushion compensation which occur when a wide-angle distortion is present in the image, a counter-distortion procedure being used to neutralise this effect.

The basic order of the procedures proposed above, in particular, the realisation of certain procedures, can be repeated with different parameters for optimisation. In the following sections we describe the processing method associated with each procedure. In each case, the distorted image I_a and the template characteristic picture Θ_T are the inputs and output is the modified partially aligned image I'_a.

B. Rotation compensation

The Characteristic Image Θ consists of a grid of correlation maxima (see Figure 13). In this case, the correct angle can be evidently defined as the one in which correlation maxima in a column are located one above another. By summing the lines of different picture rotations, the proper angle can be automatically detected in terms of that angle having the most pronounced maxima of the sum.

The Radon transform can be used to automate this procedure. It accepts a characteristic image Θ and an angle range $\Delta\alpha$ as inputs and outputs an angle-dependant line sum $\mathbf{R}$ (see Figure 15):

$$\mathbf{R} = \int_L \Theta(\mathbf{x})\,|d\mathbf{x}|$$

Each column in $\mathbf{R}$ corresponds to one particular angle of rotation. The maximum element in $\mathbf{R}$ occurs in the column corresponding to the optimal *rotation compensation angle*. When the compensation angle is known, rotation compensation can be performed for the acquired image. After rotation compensation, correlation maximums are located one above the other.

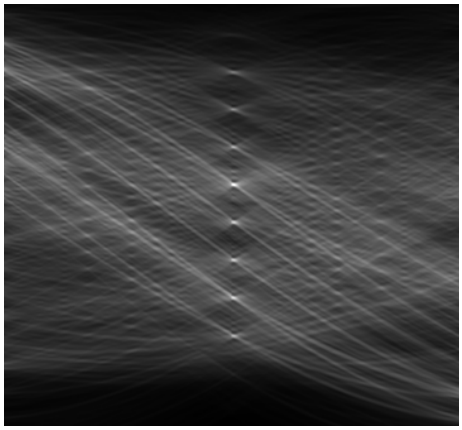

Fig. 15. Visualisation of Radon transform output $\mathbf{R}$. Each column is a line sum for a given angle of rotation. The maxima indicate the column corresponding to the rotation compensation angle.

C. Scale and shift compensation

Both scale and shift compensations for one axis have to be found simultaneously. Scaling is represented by a scale factor a and shift is described by an integer value b (in pixels). Two sets of these parameters can be found independently: the vertical (a_v, b_v), corresponding to image scaling and shifting with respect to the vertical axis and the horizontal (a_h, b_h). Only the vertical compensation will be described, horizontal compensation being performed in an entirely similiar manner.

Let the Characteristic Image Θ have dimensions $M \times N$ elements:

$$\Theta = [\Theta_{i,j}]\,,\ i = 1, ..., M,\ j = 1, ..., N$$

The *Vertical Characteristic Vector* $\mathbf{p}$ is found as a sum of all the columns of Θ:

$$\mathbf{p}_i = \sum_{j=1}^{N} \Theta_{i,j},\ i = 1, ..., M$$

This vector will have local maxima in those elements corresponding to lines in Θ where 'convolution centres' are present. The vertical characteristic vector template $\mathbf{p}^T$ is acquired from Θ_T in the same way and also has maxima in elements corresponding to the centres of each block in Θ_T. The two vectors $\mathbf{p}$ and $\mathbf{p}^T$ are then submitted to the procedure that identifies how $\mathbf{p}$ has to be scaled (a_v) and shifted (b_v) to optimally match $\mathbf{p}^T$.

Optimal matching is performed in a similar way to the cross-correlation function. For two one-dimensional vectors $\mathbf{p}$ and $\mathbf{p}^T$ a two-dimensional correlation function Φ is generated. One dimension of Φ corresponds to one of the possible scale factors a_v and the second dimension corresponds to one of the possible pixel shifts b_v as illustrated in Figure 16.

The correlation surface is acquired as follows:

1) Vector $\mathbf{p}$ is resampled with one of the scale factors a_v producing $\mathbf{p}'$.
2) For each $\mathbf{p}'$, it's cross-correlation with $\mathbf{p}^T$ is computed and the output vector is stored.
3) All output vectors for different scale factors are concatenated together string-wise to form a matrix Φ.

The maximum value in the matrix Φ indicates the best match and it's coordinates in Φ correspond to the optimum

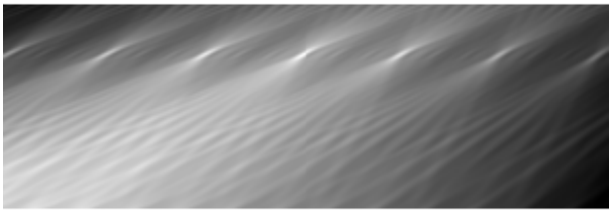

Fig. 16. Visualisation of the two-dimensional correlation function Φ showing the likeness of vectors $\mathbf{p}$ and $\mathbf{p}^T$ with different scale factors and shifts. The brightest point indicates the combination of scale a_v (row) and shift b_v (column) leading to maximum likeness.

scale factor a_v and pixel shift b_v. The same procedure is repeated for the horizontal scale a_h and shift b_h and the input image I_a is then resized by different scale factors for width and height - a_h and a_v. The pixel shift on b_v rows and b_h columns is performed for shift compensation and finally, the image is cropped to the size of Θ^T.

D. Perspective distortion compensation

After completion of the scale and shift compensation procedures, the Characteristic Image Θ has only minor differences from the template Θ_T caused by perspective and wide-angle distortions. Correlation maxima are close to the maxima positions in Θ_T. Further distortion compensation uses analytic data to predict the parameters of compensation. The procedure assumes that correlation maxima appears somewhere near the expected position, specified in Θ_T. For each expected convolution maximum in template Θ_T, some area near the maximum is analysed in the Characteristic Image Θ. The maximum element in the area is assumed to be the corresponding maximum as shown in Figure 17.

For each region, the values of *Vertical Deviation* Δy and *Horizontal Deviation* Δx are computed. The values are integer and denote the number of elements between expected and located maxima. The values are grouped together in a *Vertical Deviation Matrix* Y and *Horizontal Deviation Matrix* X:

$$\mathrm{X} = [\Delta x_{i,j}]\,,\ \mathrm{Y} = [\Delta y_{i,j}]$$
$$i = 1, ..., m,\ j = 1, ..., n$$

The perspective distortion of image I_a can be viewed as two independent perspective distortions: vertical and horizontal. We focus on the horizontal distortion here, vertical distortion compensation being implemented in a similar way.

The perspective distortion correction algorithm can be formalised in following steps:

1) The vectors $\mathbf{y}^u$ and $\mathbf{y}^l$ are taken from the first and last lines of Y.
2) For both vectors *simple linear regression* is used to detect a tendency in the $\mathbf{y}$ values, helping to generate a decision with regard to the presence and magnitude of the distortion (see Figure 18).
3) The presence of tendency indicates presence of a horizontal perspective distortion in Θ. The characteristic angles now have to be shifted vertically which uniquely defines the necessary horizontal perspective correction.

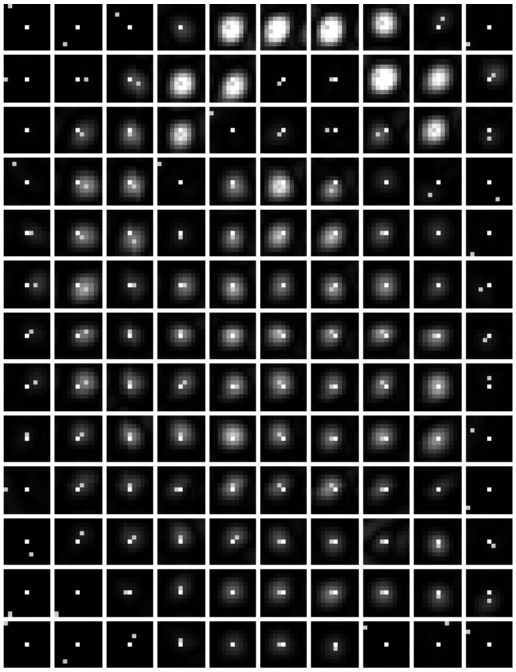

Fig. 17. A set of regions consisting of 11×11 elements around each of the expected maxima. The expected maximum position is shown as a white square (in the centre of each region). The located maximum position is shown as a light grey square.

The shift parameters are defined by the end values of the line approximation, the upper-left and upper-right hand corners being shifted by distances which are proportional to the beginning and end values of the $\mathbf{y}^u$ linear approximation, respectively (the lower-left and lower-right hand angles being proportional to the respective values of the $\mathbf{y}^l$ approximation).

The procedure is repeated twice: for horizontal and vertical correction with some minor alignment being necessary after a perspective correction.

E. Wide-angle distortion compensation

Wide-angle distortions are common in 'close-up' image acquisition. While this type of distortion is usually less pronounced than other types (as discussed above), it can still produce block displacement leading to improper watermark extraction. During barrel/pincushion distortions, parts of an image move towards/away from the centre of the image by a distance that is proportional to the third power of their initial distance from the centre L. The matrices X and Y can be used to evaluate distortion intensity.

The template characteristic picture Θ_T provides information necessary to evaluate wide-angle distortion. For each maxima that occurs in Θ_T, a characteristic vector $\vec{t}_{i,j}$ is found which 'reflects' the displacement of the maxima that occur through implementation of a synthetic distortion. A set of these vectors for each block centre is visualised in Figure 19.

Estimation of the wide-angle distortion intensity can be performed using the following steps:

1) To evaluate the presence of a wide-angle distortion the displacement vectors $\vec{d}_{i,j}$ are derived from X and Y in

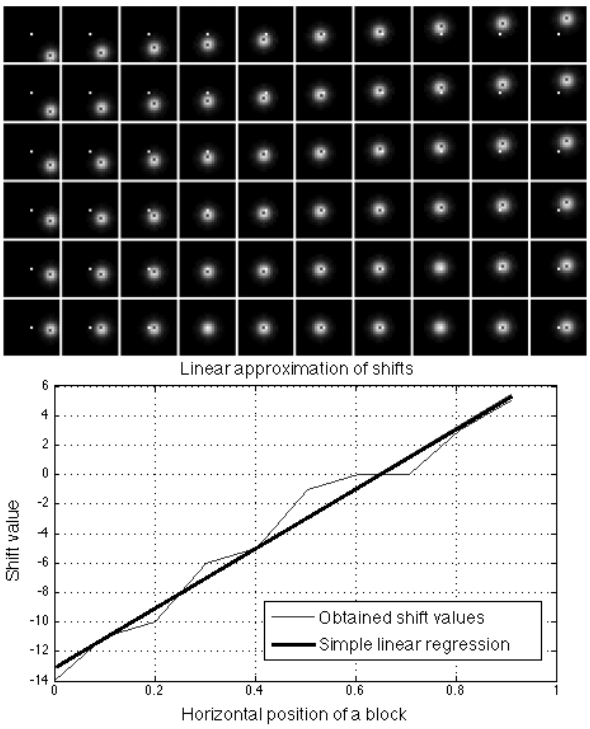

Fig. 18. Perspective distortion in an image is 'reflected' in a linearly dependent value of the vertical difference Δy between the expected and actual positions of the maxima. The linear behaviour can be utilised by linear approximation which numerically evaluates the presence of distortion in a robust manner.

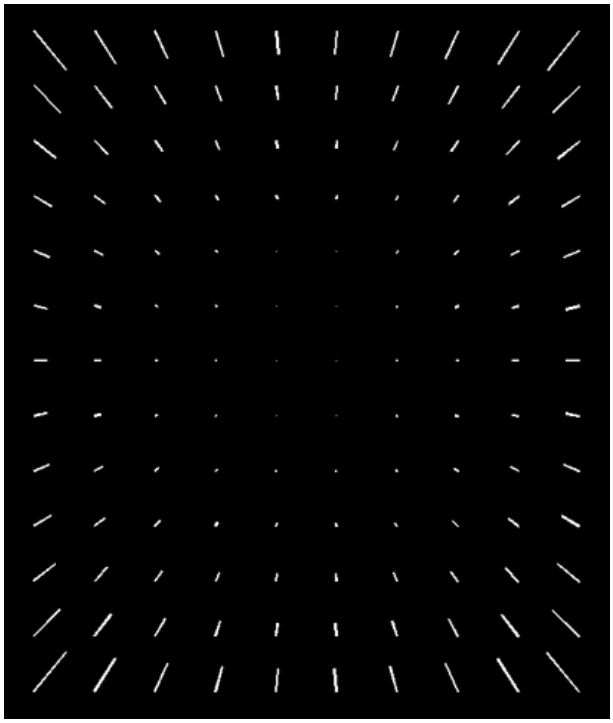

Fig. 19. Effect of barrel distortion. Each block centre is visualised with a vector $\vec{t}_{i,j}$ showing the directions in displacement for the case of a barrel distortion. In the case of a pincushion distortion, the directions are opposite.

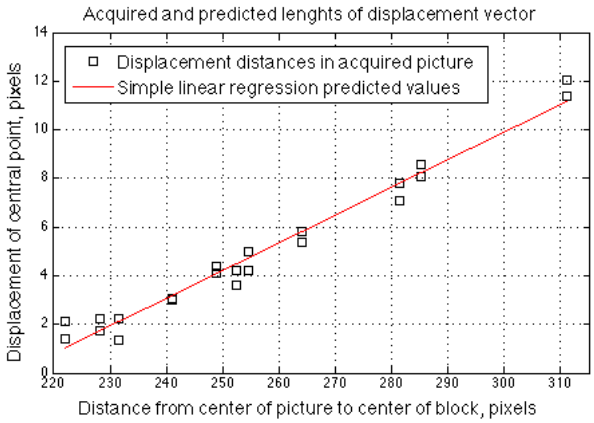

Fig. 20. Maxima displacement E′ as a function of distance from the centre of the image $\mathrm{L}_{i,j}$. The black squares represent actual values for different picture blocks. The red line represents those values acquired through linear regression.

the acquired image using the following equation

$$\vec{d}_{i,j} = (\Delta x_{i,j}, \Delta y_{i,j})$$

2) To separate the wide-angle estimate from other types of distortion, the vector $\vec{d}_{i,j}$ is projected onto the line of $\vec{t}_{i,j}$ using the equation

$$\mathrm{E}_{i,j} = |\vec{d}_{i,j}| cos(\Delta\phi_{i,j}),$$

where $\mathrm{E}_{i,j}$ is an estimation of the barrel distortion in element (i,j) and $\Delta\phi_{i,j}$ is angle between $\vec{d}_{i,j}$ and $\vec{t}_{i,j}$.

3) The array E is sorted by increasing the distance $\mathrm{L}_{i,j}$ between the centre of block (i,j) and the centre of the whole Characteristic Image Θ_T.
4) Only a part of the array E is used for analysis - E′ say, where $\mathrm{E}_{i,j} \in \mathrm{E}'$ *only if* $\mathrm{L}_{i,j} \geq 2/3 \max \mathrm{L}$. These values are located at the edge of Θ and demonstrate behaviour which is close to a linear function of L, see Figure 20.
5) Simple linear regression is applied to approximate E′ to produce the linear parameters associated with shift b and angle a. The *Barrel Compensation Parameter* is proportional to a and depends on size of Θ_T.

VII. Experimental example of implementing the automatic alignment and recovery methods

In order for the reader to appreciate the methodology reported in the previous section, in this section we report on some example results associated with an auto-alignment and recovery experiment. This section describes the result of implementing the techniques discussed so far in this paper with regard to evaluating the potential for developing an e-display/e-scan system.

We consider a container image I_c which is a full-colour RGB image of size of 800×800 pixels. Three container images are used in the experiment as shown in Figure 21. The information capacity of the embedding data $\mathbf{h}$ is 256 bits.

The experiment itself consists of following steps:

1) The watermark is embedded in the colour channels. I_c is split into 8×8 square blocks of size 100×100 pixels each. Each block is converted to $\mathrm{YC}_b\mathrm{C}_r$ colour space. Different chirplet patterns are embedded in the C_r and C_b colour channels of a block, the embedding procedure and embedding patterns being described in

Fig. 21. Container images I_c: 'Eagle' (Left), 'Lama' (Centre) and 'Chameleon' (Right).

Section V-H.

2) The watermarked image W is saved and shown on a laptop screen as shown in Figure 22.

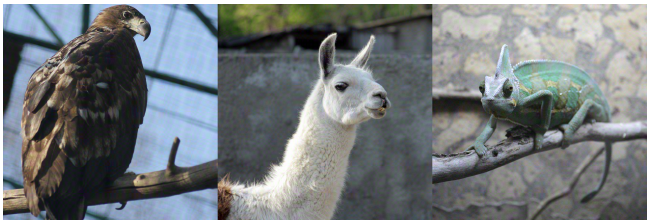

Fig. 22. Watermarked images W: 'Eagle' for $R = 0.1$ (Left), 'Lama' for $R = 0.2$ (Centre) and 'Chameleon' for $R = 0.1$ (Right).

3) A set of photos of a laptop screen showing W is taken with a phone camera. All the images acquired for this purpose are obtained at slightly different angles and distances and each image is treated separately as an acquired image I_a (see Figure 23).

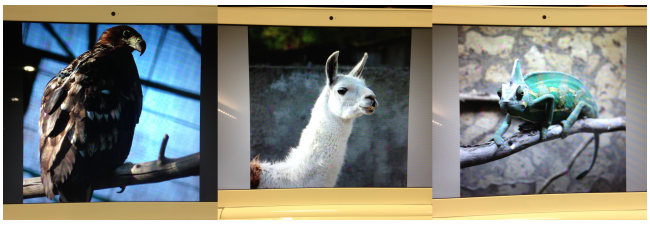

Fig. 23. Acquired images I_a - 'Eagle' (Left), 'Lama' (Centre) and 'Chameleon' (Right).

4) The characteristic image Θ is acquired from I_a as described in Section VI and the Chirplet coding method described in Section V-D used to construct the spatial embedding patterns P_v^s, an example of the characteristic image being shown in Figure 24.
5) Automatic alignment of the acquired image I_a is performed based on Θ as described in Section VI. The aligned images are shown in Figure 25.
6) The watermark $\mathbf{h}'$ is extracted from the aligned image I_a as described in Section V-I.
7) The embedding data $\mathbf{h}$ and extracted watermark $\mathbf{h}'$ are compared.

The experimental results are compounded in Table II.

VIII. Summary and Conclusion

The DCT coefficient embedding algorithm presented in this paper depends (as with all algorithms) on the specific embedding pattern used and other algorithmic parameters. However, in the context of our focus on using a DCT based approach to produce a highly resilient watermarking method, we may conclude with some common conceptual strengths and weaknesses. The strengths/weaknesses listed below are primarily concerned with the watermark robustness characteristics and do not relate to watermark capacity or visibility factors. Strengths: (i) robustness to additive noise (with a proper set of embedded patterns) and robustness to image resampling; (ii) flexible visibility and robustness characteristics through choice of different patterns and robustness to scaling (within certain limits). Weaknesses: (i) sensitivity to image shifting; (ii) sensitive to image blur (especially if the patterns include high-frequency coefficients). The sensitivity to shift is one of the principal problems associated with application of the DCT in general. Though patterns can be isolated, that have different spatial frequencies, noise robustness requires that a counter-pattern should be as close as possible to an intensity-inverted initial pattern. But due to the periodic nature of DCT-component patterns, shifted patterns can be easily recovered as counter-patterns. However, subject to the weakness listed above, the algorithm presented in this paper does provide a DCT based watermarking method that is practically applicable to print/e-display to e-scan detection that is inclusive of (marker-independent) automatic alignment. To the best of the authors knowledge, this is the first DCT-based algorithm of its type that can be used in this way.

In order to develop a system that overcomes the weakness associated with application of the DCT, we have also considered a new approach that uses a special coding kernel based on different *chirplet forms* as a binary data embedding pattern. The unique properties of chirplets (as explored in this work) allow for the achievement of very high rates of robustness to image distortion especially with regard to distortion by noise. The main aim of this work has been

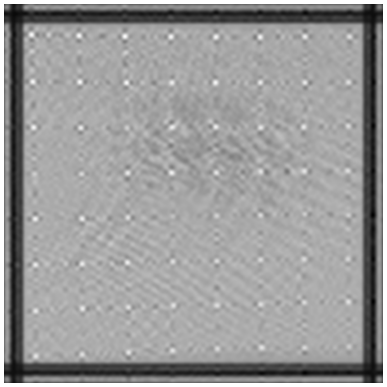

Fig. 24. Example of a characteristic image Θ which is used for auto-alignment.

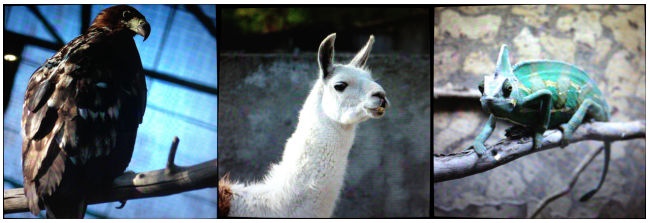

Fig. 25. Automatically aligned images - 'Eagle' (Left), 'Lama' (Centre) and 'Chameleon' (Right).

TABLE II
RESULTS OF AUTO-ALIGNMENT AND RECOVERY EXPERIMENT.

I_a	BER, %
Eagle1	16.4
Eagle2	12.5
Eagle3	9.4
Eagle4	14.1
Eagle5	11.7
Lama1	3.9
Lama2	5.4
Lama3	5.4
Lama4	29.7
Lama5	25
Chameleon1	0
Chameleon2	0
Chameleon3	0
Chameleon4	60.9
Chameleon5	0

to develop a set of numerical experiments to verify the robustness properties of the watermarking method and to define a set of optimal chirplet parameters including best estimates for the combination of minimum and maximum chirplet frequencies and optimal chirplet pairs for embedding binary data. The results show that chirplet pairs with *time reversal* provides significantly lower Bit-Error-Rates when compared to other pairs. With regard to the application of the method to image watermarking application in general, the method is shown to be adequately robust to Barrel and Rotational distortion (relatively to other image watermarking methods including the application of the Discrete Cosine and Wavelet transforms, for example) but highly robust to Blur and significantly robust to additive noise. In the latter case, and, to the best of the authors knowledge and research, the method may prove to be the most resilient of all image watermarking methods developed to date in terms of its robustness to noise. This is in keeping with previous work undertaken on chirp coding [20] including the use of multi-level chirp coding [25] and a further investigation is therefore required into the application of chirplets for the two-dimensional multi-channel watermarking of digital image using the methodology and applications discussed [26] and [27]. In this context, the procedures developed in this paper are compounded in a new 'Technology to License' [28].

ACKNOWLEDGMENTS

Jonathan Blackledge is supported by the Science Foundation Ireland Stokes Professorship Programme. Oleksandr Iakovenko is funded by the Erasmus Mundus Action II co-operation and mobility programme EWENT (East-West European Network on Higher Technical education) managed by Warsaw University of Technology, Poland. Both authors are very grateful to Dr Marek Rebow at Dublin Institute of Technology for arranging the collaborative research programme being undertaken by the authors.

REFERENCES

[1] J. M. Blacklledge, *Cryptography and Steganography: New Algorithms and Applications*. Centre for Advanced Studies Textbooks, Warsaw University of Technology, 2002.

[2] I. J. Cox, M. Miller, and J. Bloom, *Digital Watermarking*. Morgan-Kaufmann, 2002.

[3] R. J. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE: Selected Areas in Communications*, vol. 16, no. 1, pp. 474–481, May 1998.

[4] F. Petitcolas and M. Kuhn, "Information hiding: A survey," *IEEE Special Issue on the Protection of Multimedia Content*, vol. 87, no. 7, pp. 1062–1077, July 1999.

[5] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in images," *Transactions of Image Processing*, vol. 8, no. 1, pp. 58–68, 1999.

[6] J. Mintzer, F. Lotspiech and N. Morimoto, "Safeguarding digital library contents and users," *D-Lib Magazine*, December 1997.

[7] J. M. Blackledge, "Multi-algorithmic cryptography using deterministic chaos with application to mobile communications," *ISAST Trans. on Electronics and Signal Processing*, vol. 1, no. 2, pp. 23–64, 2008.

[8] J. W. Yoon and H. Kim, "Multi-algorithmic cryptography using deterministic chaos with application to mobile communications," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

[9] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers and Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[10] G. Situ and J. Zhang, "Double random-phase encoding in the fresnel domain," *Optics Letters*, vol. 29, no. 14, pp. 1584–1586, 2006.

[11] J. M. Blackllledge, *Digital Image Processing: Mathematical and Computational Methods*. Woodhead Publishing Series in Optical and Electronic Materials, 2005.

[12] J. Shen, "On wavelet fundamental solutions to the heat equation - heatlets," *Journal of Differential Equations*, vol. 161, no. 1, pp. 403–421, 2000.

[13] G. Tsaur, "Constructing green functions of the schrödinger equation by elementary transforms," *American Journal of Physics*, vol. 74, no. 7, pp. 600–606, 2006.

[14] J. M. Blackledge and O. Iakovenko, "On the application of two-dimensional chirplets for resilient digital image watermarking," in *Proc. ISSC2013*, vol. 24, 2013, pp. 1–8.

[15] J. M. Blackledge and A. R. Al-Rawi, "Application of stochastic diffusion for hiding high fidelity encrypted images," *ISAST Trans. On Computing and Intelligent Systems*, vol. 3, no. 1, pp. 24–33, 2011.

[16] J. M. Blackledge, "Steganography using stochastic diffusion for the covert communication of digital images," *IAENG International Journal of Applied Mathematics*, vol. 41, no. 4, pp. 270–298, 2011.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

[18] J. M. Blackledge and E. Coyle, "e-fraud prevention based on the self-authentication of e-documents," *Conference on Digital Society, IEEE Comp. Society*, pp. 329–338, 2010.

[19] J. M. Blackledge and A. R. Al-Rawi, "Steganography using stochastic diffusion for the covert communication of digital images," *IAENG Int. J. of Appl. Math.*, vol. 4, no. 4, pp. 270–298, 2011.

[20] J. M. Blackledge, "Digital watermarking and self-authentication using chirp coding," *ISAST Trans. on Elec. & Sig. Proc.*, vol. 1, no. 1, pp. 61–71, 2007.

[21] J. M. Blackledge and E. Coyle, "Self-authentication of audio signals by chirp coding," *Proc. DAFx09, Como, Italy*, vol. 12, no. 1, pp. 1–8, Sept. 2009.

[22] J. M. Blackledge, "Self-authentication of audio data for copyright protection," *Technology to License, Dublin Institute of Technology*, July 2009. [Online]. Available: http://www.dit.ie/hothouse/technologiestolicence/availableforlicense/ict/

[23] D. Minghui and Z. Xiuli, "A robust digital image watermarking algorithm based on chirplet transform," *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference*, pp. 86–89, October 2010.

[24] D. Minghui, Q. S. Zeng, and Y. Song, "Robust watermarking algorithm based on time-frequency chirplet," *Advanced Materials Research*, vol. 179, pp. 881–885, 2011.

[25] J. M. Blackledge and O. Farooq, "Audio data verification and authentication using frequency modulation based watermarking," *ISAST Trans. on Elec. and Sig. Proc.*, vol. 3, no. 2, pp. 51–63, 2008.

[26] J. M. Blackledge, A. R. Al-Rawi, and R. Hickson, "Multi-channel audio information hiding," *Proc. DAFx2012, York University*, pp. 309–316, September 2012.

[27] J. M. Blackledge and A. R. Al-Rawi, "Multi-channel digital rights management for audio post-production," *Technology to License, Dublin Institute of Technology*, August 2012. [Online]. Available: http://www.dit.ie/hothouse/technologiestolicence/availableforlicense/ict

[28] J. M. Blackledge and O. Iakovenko, "Two-dimensional chirplets for robust digital image watermarking," *Technology to License, Dublin Institute of Technology*, June 2013. [Online]. Available: http://www.dit.ie/hothouse/technologiestolicence/availableforlicense/ict